PH:MD
F.#2020R00093

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF ONE APPLE IPHONE CELLULAR DEVICE, MODEL IPHONE 7, IMEI NUMBER 359184070904874	**TO BE FILED UNDER SEAL** APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. 20 MJ 124

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, IGOR GAMZA, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent employed with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been a Special Agent for 4 years and have been assigned to the Cultural Property Arts and Antiquities Group since June 2019. My responsibilities include investigations of cases involving smuggling of property that is imported or exported and other cultural property crimes. I have gained expertise in this area through training in classes and daily work related to conducting these

types of investigations. As part of my responsibilities, I have been involved in the investigation of numerous cases involving importation and theft of cultural property.

3. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: my personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel. Additionally, statements attributable to individuals herein are set forth in sum and substance and in part.

4. HSI is investigating the smuggling of cultural artifacts into the United States, in violation of Title 18, United States Code, Section 545 (smuggling goods into the United States) by ASHRAF OMAR ELDARIR.

5. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

6. As set forth in Attachment A, the property to be searched is a white APPLE IPHONE CELLULAR DEVICE, MODEL IPHONE 7, IMEI NUMBER 359184070904874, hereinafter the "Device." On Wednesday, January 22, 2020, as ASHRAF OMAR ELDARIR arrived at John F. Kennedy International Airport ("JFK Airport") from Egypt, law enforcement detained the Device pursuant to its border search authority. The Device is currently in the custody of HSI within the Eastern District of New York.

7. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

APPLICABLE LAW

8. Title 19, Code of Federal Regulations, Section 141.4 requires all goods arriving at the ports of the United States to be granted "entry," or clearance, by Customs, prior to the goods being allowed to enter the commerce of the United States. As an exception to this rule, Title 19, Code of Federal Regulations, Section 143.21(a) provides that goods valued at $2,500 or less may be entered via Customs' informal entry process.

9. Pursuant to Title 19, Code of Federal Regulations, Section 148.11, persons arriving at a port of first arrival in the United States must declare all articles the person is bringing into the country to a U.S. Customs & Border Patrol ("CBP") officer. Pursuant to Title 19, Code of Federal Regulations, Sections 148.12 and 148.13, a U.S. resident returning to the United States with articles valued at over $800 must make a written declaration using Customs Form 6059-B.

10. The Convention of Cultural Property Implementation Act (19 U.S.C. § 2601, et seq.; "CPIA") imposes import restrictions on cultural property from a country of origin that has entered into an agreement with the United States under the CPIA. Pursuant to Title 19, United States Code, Section 2604, once the agreement takes force, the United States promulgates a "designated list" of archaeological or ethnological materials of the foreign country. Pursuant to the Title 19, United States Code, Section 2606, cultural property subject to such an agreement may not be imported into the United States unless the country of origin "issues a certification or other documentation which certifies that such exportation was not in violation of [its] law."

11. The United States and Egypt entered into an agreement pursuant to the CPIA in 2016. Subsequently, in 2016, the United States promulgated a regulation including a designated list of the types of Egyptian cultural property that would be subject to the CPIA's import restrictions. The designated list includes, but is not limited to, the following material dating from 5,200 B.C. through 1517 A.D.: stone, metal, ceramic or wood sculptures, vessels and containers; stone, metal or wood jewelry; stone or wood funerary objects; fiaence; glass; plaster; and cartonnage. The designated list states that wooden "[s]habti statuettes, small mummiform human figures, are especially popular."

12. Importation of stolen property into the United States, including property removed from a country in violation of a domestically enforced patrimony law, violates Title 18, United States Code, Section 2314. Article 24 of Egypt's current patrimony law, Law no. 117 of 1983 (as amended by Law no. 3 of 2010), provides that all newly discovered movable antiquities become property of the state. The law also provides that all privately owned antiquities must be registered with the Egyptian government.

13. Persons who import cultural property into the United States without the necessary export documentation from the country of origin, knowing that the property is stolen, or believing that it may be stolen because they do not have a facially valid provenance,[1] generally seek to avoid detection and targeting by Customs. Importers who seek to avoid detection and targeting by Customs often do so by means of false statements or omissions regarding the imported property, including mischaracterization of the property and

---

[1] Provenances are chronologies of an item's ownership.

its value. Such false declarations to Customs violate Title 18, United States Code, Section 545 (smuggling).

PROBABLE CAUSE

14. In January 2020, HSI began investigating ASHRAF OMAR ELDARIR, also known as OMAR ELDARIR, for violations of Title 18, United States Code, Section 545 after receiving information that ELDARIR has been selling Egyptian antiques of suspicious provenance from as early as 2013.

15. ELDARIR is a United States citizen residing in Brooklyn, New York. ELDARIR travels frequently to Egypt through JFK Airport.

16. On or about Wednesday, January 22, 2020, CBP agents, acting at the direction of HSI, stopped ELDARIR as he entered the United States from Egypt. ELDARIR was in possession of one carry-on bag and three checked suitcases that he claimed at the baggage carousel. At the Customs secondary area, CBP agents obtained a written declaration wherein ELDARIR declared that he was bringing into the country goods valued at $300. CBP agents asked ELDARIR if he was transporting any artifacts into the United States to which ELDARIR replied, "No." CBP agents examined ELDARIR's luggage, and found bubble and foam wrapped articles in all three checked suitcases. Loose sand or dirt came out of the suitcases as they were opened and as the items were unwrapped, and CBP agents noted that some of the items smelled of wet earth. A total of 590 pieces of artifacts was discovered. When asked about the various pieces of stone, wood and ceramic pieces, ELDARIR stated that they were items to decorate his two-bedroom apartment.

17. When asked whether ELDARIR had ever sold historical artifacts, ELDARIR stated in sum and substance that he had sold a few within the last two or three years.

18. CBP agents recovered from ELDARIR's luggage several documents listing previous sales of artifacts that bear ELDARIR's name, as well as documents that ELDARIR claimed were provenances created by his grandfather dating back to the 1920s. The provenances are written in Arabic on watermarked paper with stamps affixed on the top right of the documents, and two hole punches along the left-hand side. CBP agents recovered blank paper from ELDARIR's luggage that resembles the paper of the purported provenances: the paper bears the same watermark and two hole punches along the left-hand side. I also recovered 13 loose stamps similar to the ones used on the provenances from ELDARIR's luggage.

19. I have been informed by individuals familiar with Egyptian Arabic that the writing on at least some of the provenances in ELDARIR's luggage appears to be a modern Arabic writing style that was not in use during the time in which they were purported to be written. I have been also been informed by individuals familiar with Egyptian artifacts that at least some of the stamps on the purported provenances recovered from ELDARIR's luggage appear to be franked.[2]

20. CBP agents seized ELDARIR's cell phone (the Device) and manually searched its contents pursuant to the border search doctrine. The border search of the Device

---

[2] "Franked" stamps are used stamps that have been lifted off of an envelope or a letter for the purpose of reusing those stamps.

revealed evidence of smuggling by ELDARIR. For example, the Device contains photos of stamps like the ones affixed to the purported provenances. Individuals familiar with Egyptian artifacts and provenances have stated that many provenances originating from Egypt in the 1940s had stamps on them so as to add to their authenticity. The Device also contains a WhatsApp[3] album that contains numerous photos of artifacts on the ground at night. Based on my training and experience, the use of WhatsApp to share and store photos is consistent with how artifacts looters communicate, and the location of the items on the ground at night is indicative of looting. ELDARIR stated that the Device was the only cell phone he possessed at the time. The Device is currently in the custody of HSI within the Eastern District of New York.

21. Although the Device is lawfully in HSI's possession and HSI already has the necessary authority to examine the Device, to ensure that a search of the Device would comply with the Fourth Amendment and other applicable law, I now submit this affidavit seeking a warrant to search the Device for evidence related to the smuggling of goods into the United States.

TECHNICAL TERMS

22. Based on my training and experience, I use the following technical terms to convey the following meanings:

---

[3] WhatsApp Messenger ("WhatsApp") is an instant messaging application designed for use on smartphone devices.

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard

drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that

computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

23. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that

establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

27. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

28. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

REQUEST FOR SEALING

29. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into criminal organizations and not all of the

targets know about this investigation. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness, including by giving an opportunity for targets to flee from prosecution and destroy evidence.

Respectfully submitted,

IGOR GAMZA
Special Agent
United States Department of Homeland Security, Homeland Security Investigations

Subscribed and sworn to before me
on February 6, 2020:

THE HONORABLE ROANNE L. MANN
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

The property to be searched is a white APPLE IPHONE CELLULAR DEVICE, MODEL IPHONE 7, IMEI NUMBER 359184070904874, hereinafter the "Device." The Device is currently in the custody of HSI within the Eastern District of New York. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of 18 U.S.C. § 545 since January 1, 2013, including:

   a. lists of customers and related identifying information;

   b. types, amounts, descriptions, and prices of artifacts sold as well as dates, places, and amounts of specific transactions, including but not limited to invoices;

   c. any information related to sources of artifacts (including names, addresses, phone numbers, or any other identifying information);

   d. any information recording ASHRAF OMAR ELDARIR's schedule or travel;

   e. all bank records, checks, credit card bills, account information, and other financial records;

   f. correspondence with potential buyers and sellers of artifacts; and

   g. photographs of artifacts, documents, and stamps.

2. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

3. Records evidencing the use of the Device's Internet Protocol address to communicate with customers, including:

   a. records of Internet Protocol addresses used;

   b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user

entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.